Grupo 2:
Constanza Victoriano
Benjamín Jiménez
Agostina Ducret
Felipe carrasquilla
Facundo Peñaloza
Johana Ruiz
Verónica Jiménez

Nota : <BackdoorDiplomacy: actualizando de Quarian a Turian, un backdoor utilizado contra organizaciones diplomáticas | WeLiveSecurity>

¿Qué tipo de amenaza es?
Backdoor virus

¿Cómo comienza y cómo se propaga esta amenaza?
Su metodología de ataque inicial consiste en explotar aplicaciones vulnerables expuestas a Internet en servidores web, con el fin de droppear y ejecutar un webshell. Después del compromiso, a través del webshell, BackdoorDiplomacy utiliza software de código abierto para el reconocimiento y la recopilación de información, y hace uso de la técnica DLL search order hijacking para instalar su backdoor.

¿Hay más de una amenaza aplicada ?

Los virus que se introducen mediante backdoors a menudo tienen capacidades destructivas adicionales: realizan capturas de pantalla, registran de pulsaciones de teclas o infectan y cifran archivos. Una puerta trasera permite al intruso crear, eliminar, renombrar, editar o copiar cualquier archivo, ejecutar diferentes comandos, cambiar cualquier configuración del sistema, borrar el registro de Windows, ejecutar, controlar y terminar aplicaciones, o instalar nuevo malware.

Asimismo permite al atacante controlar los dispositivos de hardware, modificar la configuración relacionada, reiniciar o apagar un equipo sin pedir permiso y robar datos personales confidenciales, contraseñas, nombres de inicio de sesión, detalles de identidad y documentos valiosos.

Algunos ataques de puerta trasera son rentabilizados registrando la actividad de los usuarios y rastreando los hábitos de navegación web o infectando archivos, dañando el sistema y corrompiendo las aplicaciones.

¿Qué solución o medida recomendarían ?
recomendación: recurrir a una herramienta para su eliminación automática; los antivirus cuentan con esta opción, de manera que cuando encuentran un virus lo marcan para su posterior eliminación. Este proceso viene explicado paso a paso por el propio antivirus que estemos usando, por lo que generalmente es sencillo de hacer. También podemos recurrir a otros programas de limpieza, como CCleaner o Malwarebytes Anty-malware, para usarlos tras realizar el análisis con el antivirus.